MATH 240: Discrete Structures - Assignment 3

Liam Scalzulli
liam.scalzulli@mail.mcgill.ca

October 30, 2022

Problem 1

Proof. Assume $2^n - 1$ is prime.

Let $\sigma(n)$ be a function that computes the sum of all divisors of a given number n.

Then $\sigma(2^n - 1) = 2^n$ since the only divisors of $2^n - 1$ are 1 and $2^n - 1$ as a result of $2^n - 1$ being prime.

Moreover, we have $\sigma(2^{n-1}) = 2^n - 1$ as the divisors of 2^{n-1} are all powers of 2 up to and including 2^{n-1}.

Putting it all together:

$$\begin{aligned}
\sigma(2^{n-1}(2^{n-1}))) &= \sigma(2^{n-1})\sigma(2^n - 1) \\
&= (2^n - 1)(2^n) \\
&= 2(2^{n-1})(2^n - 1)
\end{aligned}$$

Therefore $2^n - 1(2^n - 1)$ is a perfect number. $\square$

Problem 2

Step 1: Find $148^{-1} \pmod{421}$

Compute the steps of the Euclidean GCD algorithm:

$$
\begin{aligned}
421 &= 2 \times 148 + 125 \\
148 &= 1 \times 125 + 23 \\
125 &= 5 \times 23 + 10 \\
23 &= 2 \times 10 + 3 \\
10 &= 3 \times 3 + 1
\end{aligned}
$$

Roll back the steps to find $s, t \in \mathbb{Z}$ such that $1 = 421s + 148t$

$$
\begin{aligned}
1 &= 1(10) - 3(3) \\
&= 1(10) - 3(23 - 2(10)) \\
&= 7(10) - 3(23) \\
&= 7(125 - 5(23)) - 3(23) \\
&= 7(125) - 38(23) \\
&= 7(125) - 38(148 - 1(125)) \\
&= 45(125) - 38(148) \\
&= 45(421 - 2(148)) - 38(148) \\
&= 45(421) - 128(148)
\end{aligned}
$$

So $1 = 45(421) - 128(148)$, we then get $1 = -128(148)$, hence $148^{-1} \pmod{421} \equiv -128 \equiv 293 \pmod{421}$.

Step 2: Solve $148x \equiv 12 \pmod{421}$

$$
\begin{aligned}
148x &\equiv 12 \pmod{421} \\
x &\equiv 12 \times 293 \pmod{421} \\
&\equiv 3516 \pmod{421} \\
&\equiv 148 \pmod{421}
\end{aligned}
$$

Problem 3

Recall: $a^{p-1} \equiv 1 \text{ (mod p)}$

(a)

$$\begin{aligned}
2409^{1335} \pmod{19} &= 2409^{(18 \cdot 74)+3} \pmod{19} \\
&= 2409^{3} \pmod{19} && [2409 \equiv 15 \pmod{19}] \\
&= 15^{3} \pmod{19} \\
&= 3375 \pmod{19} \\
&= 12 \pmod{19}
\end{aligned}$$

(b)

$$\begin{aligned}
7^{42806} \pmod{349} &= 7^{(123 \cdot 348)+2} \pmod{349} \\
&= 7^{2} \pmod{349} \\
&= 49 \pmod{349}
\end{aligned}$$

Problem 4

(a)

$$\begin{aligned}\hat{M} &= M^p \text{ mod n}\\ &= 4^5 \text{ mod } 91\\ &= 1024 \text{ mod } 91\\ &= 23\end{aligned}$$

(b)

$$\begin{aligned}x &= p^{-1} \text{ mod } (q_1 - 1)(q_2 - 1)\\ &= 5^{-1} \text{ mod } 72\end{aligned}$$

Compute the steps of the Euclidean GCD algorithm:

$$\begin{aligned}72 &= 14 \times 5 + 2\\ 5 &= 2 \times 2 + 1\end{aligned}$$

Roll back the steps to find $s, t \in \mathbb{Z}$ such that $1 = 5s + 72t$

$$\begin{aligned}1 &= 5 - 2(2)\\ &= 5 - 2(72 - 14(5))\\ &= 29(5) - 2(72)\end{aligned}$$

So we see that $x = 29$, since $p \cdot 29 \equiv 1 \text{ mod } 72$.

(c)

$$\begin{aligned}M &= \hat{M}^x \text{ mod n}\\ &= \hat{M}^{29} \text{ mod } 91\\ &= 23^{29} \text{ mod } 91\\ &= 4\end{aligned}$$